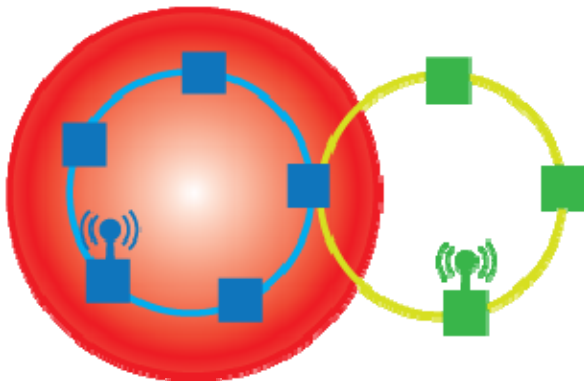


VIRTUAL Local Area Networks



The Issue

The initial installation of a Local Area Network (LAN) generally involves deploying category 5 cabling throughout the physical premises and connecting them to one or more network switches. This is satisfactory for an organization with a simple need for connecting multiple computers to the Internet (via a router), sharing networked printers, sharing files via network attached storage, or a server, email and the like.

A challenge arises when different levels of security are needed because of sensitive information

residing on a corporate server, or a wish to provide network access to vendors, contractors or guests. A relatively difficult, and usually costly way to provide this type of network segregation would be to physically separate the various network groups.

The purpose of this document is to illustrate the benefits that accrue to an organization through the use of Virtual Local Area Networks (VLAN) to achieve network segregation, both in terms of expense reduction and ease of management.

What is a VLAN?

During the design stages of a traditional LAN, the physical location of where computers will be located can be an initial objective. Combine this with sensitive data networks that need physical separation and it becomes imperative that everything is carefully planned as there will be little room for change after installation. If two (or more) networks are required to separate sensitive data for security purposes, this requires additional physical sets of wire to be installed and maintained.

Equally, when additional network capacity is required, new cable has to be installed multiple times for physically separated networks, so the physical constraint on computer relocation becomes a problem. All of these factors add costs to both the installation and day to day management of networks. By using VLANs, we can allow for these changing requirements.

Where would I use a VLAN?

With the use of Virtual LANs or VLANs (802.1q), we can use the actual switch to overcome many of these issues and enhance both the management of our networks and ultimately the performance.

A VLAN is a software controlled network; it behaves as though it is connected by the same cable as a traditional network although physically it may be separated across different segments of the network. This logical grouping of computers allows far simpler configuration even if the nodes are spread over a large geographical area.

USRobotics offers two types of VLAN with our range of smart switches – **Port Based VLANs and Packet Based VLANs.**

With *Port Based VLANs*, each port on the switch can be allocated to a VLAN or VLAN group. Any node connected to a port will automatically have membership to the VLAN that the port is associated to and will not have access to any resource or VLAN not exposed to that port. This effectively creates a network per port or groups of ports as if they were wired separately.

Port based VLANs allow two nodes to be attached to the switch, share the same physical wiring yet ultimately be completely separated.

If we take the example of a school, it is imperative that the pupils do not have access to the teacher's resources. Using traditional networking, the installation of two physical networks is the only method of guaranteeing mobility for the teachers whilst maintaining network security. This is of course expensive to install and maintain.

Benefits of a VLAN

If VLANs are introduced into the same scenario, two logical networks can be created that are separate from each other while utilising one set of switches and physical wiring.

If a classroom has to be rearranged, the physical wiring can stay in place and the switch can be configured to reflect the move by the simple changing of the port settings. Where the teacher may have been hardwired into port 1 of the switch which belonged to the teachers VLAN, and they have now been moved to port 2, the simple changing of the VLAN setting from port 1 to 2 will enable the teacher to stay on the same logical network. This doesn't even require a trip to the server room for the administrator as the configuration can be made on the switch from any machine on the network since no physical changes are being made.

The use of VLANs can be extended from one switch to another allowing it to be continued across an entire network thus further removing physical constraints from a network. An employee can be moved from building to building or from one LAN segment to another while remaining on the same VLAN.

This becomes particularly relevant when we consider *Packet Based VLANs*, which is the second type of VLAN that the USRobotics Courier Smart Switches offer.

When data is transmitted through a network, it is sent in the form of data packets which are then packed into frames for ease of transmission. As these frames pass through the switch, destination information is attached (tagged) which identifies which VLAN the data is destined for.

The benefit of packet based VLANs is the removal of port dependency because as the tagging information is placed in the frame, multiple VLANs can be transmitted from a single port.

The Network Interface Card (NIC) on the end node is then configured to retrieve only packets that have their VLAN information included.

Because each frame is tagged by the switch with its VLAN membership information, computers can be moved anywhere on the network yet still have access to the same resources. When using Packet Based VLANs, a computer can be moved without having to reconfigure any part of the network as it will simply listen for data that is transmitted with its tagged information.

This completely eliminates any physical limitation of a network. Whole departments can be moved efficiently around a network with no disruption or costly re-wiring. Computers needing different resources that traditionally would require re-wiring can be located next to each with no change to the wired infrastructure.

Where logical networks are created as opposed to physically dependant networks, administrators can further group departments by subnets and IP address ranges even when the nodes are physically diverse. With this approach enhanced further by the centrally managed switches, VLANs offer a more efficient networking option.

As multiple networks can be transmitted through a single switch port using packet based IEEE802.1q, when used with the USRobotics Professional Access Point (USR805453A) it is also fully possible to transmit up to four wireless networks simultaneously with just one access point.

This further removes physical limitation and extends the VLAN solution allowing wireless mobility. The USRobotics Professional Access Point supports up to four distinct wireless networks (SSIDs), each with their own security settings.

If this is applied to the school scenario, the teacher's network can be transmitted with the highly secure WPA2 protocol which creates a secure and robust wireless network while the pupil's network can be secured with WEP to ensure compatibility, while maintaining the required separation. All of the resources are still kept distinctly separate and secure while taking advantage of wireless flexibility.

www.usr.com

USRobotics®